U.S. Department of Transportation

Federal Aviation Administration

Advisory Circular

Subject: ACCEPTANCE AND USE OF ELECTRONIC SIGNATURES, ELECTRONIC RECORDKEEPING SYSTEMS, AND ELECTRONIC MANUALS

Date: XX/XX/01 **AC No: 120-ES**

Initiated By: AFS-300 **Change:**

DRAFT

1. PURPOSE. This advisory circular (AC) provides guidance on the acceptance and use of electronic signatures to satisfy operational and maintenance requirements. This AC also provides guidance on the acceptability of electronic recordkeeping systems and electronic maintenance manuals, including inspection procedures manuals and/or quality assurance manuals required by Title 14 of the Code of Federal Regulations (14 CFR).

2. CANCELLATION. AC 120-69, Use of CD-ROM Systems, dated 8/14/97, is cancelled.

3. RELATED READING MATERIALS.

a. Title 14 CFR: Parts 43, 91, 119, 121, 125, 129, 133, 135, 137, and 145.

b. Federal Aviation Administration (FAA) Orders. Copies of the following documents may be purchased from: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.

(1) Order 8300.10, Airworthiness Inspector's Handbook,

(2) Order 8400.10, Air Transportation Operations Inspector's Handbook,

(3) Order 8000.9, Use of Electronic Technology and Storage of Data.

4. DEFINITIONS. For the purposes of this AC, the following definitions apply:

a. Authentication. The means by which a system validates the identity of an authorized user. These may include a password, a personal identification number (PIN), a cryptographic key, a badge, or a stamp.

b. Digital Signature. Digital signature technology is the foundation of a variety of security, e-business, and e-commerce products. This technology is based on public/private key

cryptography, digital signature technology used in secure messaging, public key infrastructure (PKI), virtual private network (VPN), web standards for secure transactions, and electronic digital signatures.

c. Electronic Signature. An electronic sound, symbol, or process attached to, or logically associated with, a contact or other record and executed or adopted by a person with the intent of electronically identifying and authenticating an individual entering, verifying, or auditing computer-based records. An electronic signature combines cryptographic functions of digital signatures with the image of a person's handwritten signature or some other form of visible mark that would be considered acceptable in a traditional signing process, authenticates data with a hashing algorithm, and provides permanent secure user-authentication.

d. Signature. Any form of identification used as a signature to attest to the completion of an act and authenticate a record entry must be traceable to the person making the entry and must be handwritten, or part of an electronic signature system or other form acceptable to the Administrator.

5. FOCUS. This AC applies to air carriers using electronic signatures under 14 CFR Part 121 or Part 135. Persons performing maintenance or preventive maintenance under 14 CFR Part 43, operators under 14 CFR Part 91 or Part 125 and repair stations under 14 CFR Part 145 may use the criteria of this AC to the extent that its provisions are pertinent to their operations.

6. BACKGROUND. A recent amendment to Title 44 of the United States Code, chapter 35, requires Federal agencies to implement procedures for managing their information resources in a manner that will improve the utility of information for users and for archiving information in electronic format. In addition, the Electronic Signatures in Global and National Commerce Act (ESign) provides that Federal agencies give legal effect to electronic signatures. This AC represents one part of the FAA's effort to comply with that mandate. Reference <http://www.sec.gov/rules/proposed/33-7955.htm>

a. Before the enactment of ESign of June 30, 2000, the regulations governing the use of signatures to satisfy maintenance and operational requirements did not reflect current advances in information storage and retrieval technology. These earlier rules were developed at a time when the use of electronic media for the storage and retrieval of data was neither available to, nor contemplated by, the aviation industry or the FAA.

b. As the complexity of aircraft design, operations, and maintenance processes increased, the number of records and documents generated and required to be retained by aircraft owners, operators, manufacturers, and repair facilities expanded dramatically. The development of electronic information storage and retrieval systems has significantly enhanced the ability of the aviation industry not only to meet FAA record-retention requirements, but also to manufacture, operate, and maintain today's highly complex aircraft and aircraft systems in a demanding operational environment.

c. Previous regulations restricted the full implementation of electronic information storage and retrieval systems because digital electronic signatures were not permitted on any record or

document that required the affixation of a signature. Any record or document produced electronically continued to be authenticated using a non-electronic signature. This practice greatly diminished the benefits inherent in the use of any electronic system.

d. The Office of Management and Budget (OMB), Executive Office of the President, issued OMB Circular A-130, Management of Federal Information Resources, which required the FAA and other government agencies to recognize the limitations imposed by these restrictions on the use of electronic signatures and revised the regulations governing the use of signatures to permit the use of electronic signatures on maintenance and operational records. Owners, operators, and maintenance personnel may now implement complete electronic recordkeeping systems because the earlier requirement to authenticate these documents using non-electronic signatures has been eliminated. Such systems may now be used to generate Aircraft records such as load manifests, dispatch releases, maintenance task cards, aircraft maintenance records, flight releases, airworthiness releases, and flight test reports that can be authenticated using a digital electronic signature.

e. Acceptance of digital electronic signatures will encourage the use of electronic maintenance logbooks to comply with record retention and record entry requirements because maintenance, preventive maintenance, rebuilding, and alteration records may now be authenticated using a digital electronic signature. Digital electronic signatures will also simplify the application process for a Designated Alteration Station (DAS) or delegation option authorization, and speed up the process by which changes are made to a DAS procedure manual or quality control system.

f. The use of digital electronic signatures enhances the ability to identify a signatory and helps to eliminate the tractability difficulties associated with illegible handwritten entries and the deterioration of paper documentation.

7. DISCUSSION.

a. General. Before recent changes to permit the use of digital electronic signatures, a handwritten signature was the primary means by which an individual could comply with the requirement for a signature on any required record, record entry, or document. Although an electronic signature may be essentially a new form of signature, its purpose is identical to that of a handwritten signature or any other form of signature currently accepted by the FAA. The handwritten signature is universally accepted because it has certain qualities and attributes that should be preserved in any electronic signature. Therefore, to be considered acceptable, an electronic signature should possess those qualities and attributes intrinsic to a handwritten signature that guarantee its authenticity.

b. Forms of Electronic Signatures. An electronic signature may be in the form of a digital signature, a digitized image of a paper signature, a typed notation, an electronic code, or any other unique form of individual identification that can be used as a means of authenticating a record, record entry, or document. Users of electronic signatures should be aware that not all identifying information found in an electronic system may constitute a signature. For example, the entry of an individual's name in an electronic system may not constitute an electronic

signature. Other guarantees commensurate with those of a handwritten signature should be provided.

c. Attributes of an Acceptable Electronic Signature.

(1) Uniqueness. A digital electronic signature should retain those qualities of a handwritten signature that guarantee its uniqueness. A signature should identify a specific individual and be difficult to duplicate. A unique signature provides evidence that an individual attests to a statement. An electronic system cannot provide a unique identification with reasonable certainty unless the identification is difficult for an unauthorized person to duplicate. An acceptable method of proving the uniqueness of a signature is an identification and authentication procedure that validates the identity of the signatory. For example, an individual using a digital electronic signature should be required to identify himself or herself, and the system that produces the digital electronic signature should then authenticate that identification. Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes. These codes could be encoded onto badges, cards, cryptographic keys, or other objects. Systems using PINs or passwords memorized by an individual could also serve as an acceptable method of ensuring uniqueness. Additionally, a system could also use physical characteristics, such as a fingerprint, handprint, or voice pattern as a method of identification and authorization.

(2) Significance. An individual using a digital electronic signature should take deliberate and recognizable action to affix his or her signature. Acceptable, deliberate actions for creating a digital electronic signature include, but are not limited to: badge swipes, signing an electronic document with a stylus, inputting a specific keystroke(s), or using a digital signature.

(3) Scope. The scope of information being attested to via a digital electronic signature should be made clear to the signatory and to subsequent readers of the record, record entry, or document. While handwritten documents use the physical proximity of the signature to the information in order to identify those items attested to by a signature, electronic documents may not use the position of a signature in the same way. It is therefore important to clearly delineate the specific sections of a record or document that are affected by a signature from those sections that are not affected. Acceptable methods of delineation of the affected areas include, but are not limited to: highlighting, contrast inversion, or the use of borders or flashing characters. In addition, the system should notify the signatory that the signature has been affixed.

(4) Signature Security. The security of an individual's handwritten signature is maintained by ensuring it is difficult for another person to duplicate or alter it. A digital electronic signature should maintain an equivalent level of security. Due to the reproduction capability inherent in an electronic system, an electronic system used to produce a signature should restrict the ability of any person to cause another individual's signature to be affixed to record, record entry, or document. Such a system enhances safety by precluding an unauthorized person from certifying required documents, such as an airworthiness release.

(5) Nonrepudiation. A digital electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document. The

more difficult it is to duplicate a signature, the greater the likelihood that a signature was created by the signatory. Those security features of an electronic system that make it difficult for another person to duplicate a signature or alter a signed document tend to ensure that a signature was indeed made by the signatory.

(6) Tractability. A digital electronic signature should provide positive tractability to the individual who signed a record, record entry, or any other document.

d. Other Acceptable Forms of Signatures. Although this AC specifically addresses digital electronic signatures, other types of signatures, such as a mechanic's stamp may also be acceptable to the Administrator. If a form of identification other than a handwritten signature is used, access to that identification should be limited to the named individual only. For example, a mechanic's stamp should be secured when not in use by the individual whom the stamp identifies. Similarly, a computer entry used as a signature should have restricted access that is limited by an authentication code that is changed periodically. Access to issued stamps or authentication codes should be limited to the user. Although a signature may take many forms, the FAA emphasizes that all electronic entries may not necessarily satisfy the criteria that would qualify an electronic entry as an acceptable signature.

e. Restrictions on the Use of Digital Electronic Signatures. Owners, operators, and maintenance personnel should note that provisions regarding the acceptability of electronic signatures are not found in 14 CFR Part 1, which is of general applicability, but rather in Parts 43, 91, 119, 121, 125, 129, 133, 135, 137, and 145, which are of more limited applicability. Specific requirements for the use of signatures are found throughout the regulations. These requirements affect areas other than those discussed in this AC. Digital electronic signatures may not be considered acceptable in these areas and, therefore, should only be used to satisfy maintenance and operational requirements, unless otherwise permitted. Although the acceptance of digital electronic signatures will foster the use of electronic recordkeeping systems, the FAA continues to accept the use of paper documents to satisfy current regulatory requirements.

f. Compliance with Other Regulatory Requirements. The FAA notes that, although it now permits the use of digital electronic signatures, any electronic system used to generate the required documents and records must continue to meet current regulatory requirements. A proper signature affixed to an improperly created document still results in a document that does not meet regulatory requirements. In any recordkeeping system, methods and procedures used to generate an electronic signature must therefore meet all regulatory requirements in order to be used by owners, operators, or maintenance personnel.

g. Announcing Intent to Use Digital Electronic Signatures. Persons intending to use digital electronic signatures should consult with their local Flight Standards District Office (FSDO) before implementing electronic systems. A written description of how digital electronic signatures will be used in maintenance and operational activities should also be submitted. Inspectors will review the digital electronic signature methods proposed. After finding the methods acceptable, the FAA will add a statement to the operator's operation specifications, identifying the location of the manual instructions for use of electronic systems. In

the case of a Part 91 operator, the local FAA office will provide a letter accepting the procedures for use of an electronic system.

8. ELECTRONIC RECORDKEEPING SYSTEMS.

a. OMB Circular A-130 allows individuals or entities that deal with agencies the option to perform the following functions electronically when practical: submit information or transact with those agencies, and to maintain records. The Act specifically states that electronic records and their related electronic signature are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. When constructing an electronic recordkeeping system, the following elements must be considered and addressed in a section of the operator's manual or within the directions for use of the electronic system and made available to each person responsible for utilizing the system.

> **NOTE: Contents of a recordkeeping system for an air carrier certificate holder can be found in the appropriate regulations as well as in FAA Order 8300.10, volume 2, chapter 71.**

(1) Security.

(a) The electronic system must protect the information confidentially.

(b) The system must ensure that the information is not altered in an unauthorized way.

(c) A corresponding policy and management structure must support the hardware and software that delivers the information.

(2) Before introducing an electronic system, a computer operation procedures manual must be established. The manual must include the following:

(a) Procedures for making required records available to the National Transportation Safety Board (NTSB) and/or FAA personnel, a company employee, or a representative who is acutely familiar with the computer system to assist in accessing the necessary computerized information. This procedure and computer system must be capable of producing paper copies of the viewed information at the request of the Administrator.

(b) A procedure for conducting a review of its computerized personal identification codes system to ensure that it will not permit password duplication.

(c) A procedure that establishes an audit of the computer system every 60 days to ensure the integrity of the system.

(d) An audit procedure that is designed to ensure the integrity of each computerized workstation.

(e) Procedures that describe how it will ensure that the computerized records will transmit to its customers or to another operator.

(f) A procedure that ensures that, in cases involving records that are required to be transferred with an aeronautical product, the new owner/operator has the required information in a format acceptable to the new owner/operator, either electronically or on paper.

(g) Guidelines for the use of electronic signatures for authorized representatives and access to appropriate records by authorized representatives of the owner/operator.

(h) A description of the training procedure and requirements necessary to authorize access to the computerized system.

b. The user must provide a copy of the procedures to be used for implementing an electronic recordkeeping system to the FAA Certificate-Holding District Office (CHDO) or the FAA office with oversight jurisdiction.

c. Once satisfied with the manual, the FAA will make the appropriate entry on the operator's operation specifications. In the case of a Part 91 operator, the FAA CHDO will forward a letter of acceptance/rejection to the owner/operator (See Appendices 1 and 2).

9. ELECTRONIC MANUALS.

a. Background.

(1) The Federal Aviation Regulations permit the preparation, use, and retention of the maintenance portion of a certificate holder's manual(s) or operator's maintenance manual(s) in electronic format if that format is acceptable to the Administrator. The FAA has determined that electronic storage and retrieval of the information contained in those manuals that are in a CD-ROM, on-line, or other electronic media format offer improved data accessibility, quality control, and speed distribution over paper or microfilm-based information storage systems. These improvements result in enhanced safety and a reduced economic burden on industry and government by providing users with more rapid access to information at a reduced cost. These improvements also provide industry with a means to enhance the manner in which it presents the technical data contained in a certificate holder's or operator's manual(s) by facilitating the use of media formats (e.g., visual displays, video, graphic files, audio, animation, and computer files) that are incompatible with the use of paper or microfilm-based manuals.

(2) Any acceptable electronic manual system must deliver to the user the information contained in the system with at least the same degree of accuracy and integrity afforded by the use of a system based on a paper or microfilm format. The use of electronic media for the storage and retrieval of technical data does not relieve a certificate holder/operator from compliance with other regulatory requirements pertaining to the currency, completeness, use, or availability of the technical data.

(3) When developing and implementing an electronic maintenance manual system, the following must be taken into consideration:

(a) Specification and installation of computing platforms, hardware, software, and retrieval tools. The computing platform hardware, software, and retrieval tools should be able to store and retrieve the technical data contained in the manual under conditions of normal operation and use. The system should not permit unauthorized modification of the data it contains.

(b) Ongoing maintenance and support of the computing platform, including provisions for outages and necessary alternative retrieval services. Although maintenance and support for the system may be provided by sources independent of the certificate holder or operator, responsibility for compliance with all regulatory requirements cannot be delegated.

(c) Distribution of technical data to authorized users. The certificate holder or operator should ensure that required personnel are provided with copies of manuals contained in an electronic system or that the manuals are made available to the personnel, as appropriate. The procedures for the distribution of the manual and the included technical data need not differ substantially from the procedures used for the distribution of information contained in paper or microfilm manuals. Certificate holders and/or operators may use their current manual distribution system for the distribution of manuals in an electronic format.

(d) Creation and distribution of any incremental or temporary revision required between scheduled revisions. The certificate holder or operator should establish procedures to verify that revisions to the technical data contained in the maintenance portion of its manual are current and complete and have been authorized by the appropriate authority before distribution.

(e) Accessibility by the FAA or NTSB. The electronic manual system must permit any authorized representative of the Administrator or the NTSB to retrieve, print, or view the information contained in any required manual that is now maintained in electronic format. If a certificate holder or operator is required to provide information to the FAA or NTSB, the certificate holder or operator must be able to provide the record in a format that is usable by the requested agency.

(f) User Instructions. A certificate holder or operator should provide the user with information describing the use and operation of the electronic system to include: information and instructions for using publications, reference information, and system administration information. These instructions need not be in paper form. They may consist of electronic, context-sensitive help; on-line or system responses to specific operator queries; telephonic or electronic access to a designated assistance line; or other information included in the electronic system.

(g) Training. The certificate holder or operator should establish a training program for employees or contractors who will use the electronic system. The subject matter and objectives of the training provided should vary depending on the employees or contractor job responsibilities and function level within the organization. Customer training should include security awareness and policy and procedures for system operation. Acceptable methods of

providing this training may include, but are not limited to, classroom instruction, on-line or system tutorials, user guides, and simulated problem solving exercises. Any training program should define minimum competency criteria and the method for demonstration of user competence.

(h) Enhancements. Additional features such as text searching, hypertext links, or other enhancements that facilitate access to the information are generally not required for a system to be considered acceptable.

b. Functional Considerations.

(1) Any electronic system should provide the user with the ability to retrieve the technical data contained within any manual stored in the system. Any electronic system should have the ability to access, navigate, and retrieve applicable information at a computer workstation. The user accesses this information via specific methods provided by the system. Electronic information stored in the system may occur in either a stand-alone or a shared environment.

(2) The content of a manual contained in the electronic system must be available and able to be viewed by the user. When the requested information is presented by the system, the results should be capable of being displayed on a computer screen or comparable device. If connected to a paper printer, the electronic system should have the ability to output in paper form any information contained in a manual stored within the system. The format of any printed output from the system should clearly identify the information presented and easily correlate to corresponding information contained in a printed version of the manual.

c. Revision Control Procedures.

(1) Validation of Revision Control Procedures. Certificate holders and operators should establish revision procedures to audit the revision process and ensure that the contents of the electronic system are current and complete. The revision control procedures for electronic manual data may be similar to the revision control procedures used for other storage media.

(2) Revision Transmittal Letter/Release Notes. Many certificate holders and operators frequently use internal distribution documents that specify the current revision number and date for each revision. This document is sometimes provided separately, in which case it conveys revision number and dates with applicable instructions to the users. A user can inspect and review this documentation to determine data currency.

(3) Data Currency Audit. Certificate holders and operators should establish procedures to ensure the currency of the technical data (regardless of the storage media) that they use. Certificate holders and operators must ensure that all electronic storage media contain the current revision and associated revision dates. With electronic media, page level insertion audits of manuals by the user may no longer be necessary to ensure information currency.

(4) User Responsibility. Users of information obtained from electronic manuals systems, especially the data output in printed form, should ensure that the output was obtained from the most current manual data available to the certificate holder or operator.

d. Special Considerations in Displaying Output.

(1) Data Content and Output Form.

(a) The capability and advancements of electronic retrieval systems may cause information retrieved from a manual stored in an electronic system to be displayed in a different format than it appears on paper or microfilm pages. The information should be identical in content regardless of output of form.

(b) Any display output should be readily traceable to its original source. From the displayed output, the user should be able to obtain: the manual title; applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model; effectiveness of the data; and revision simultaneously displayed with the technical data (e.g., on the computer screen). This information must be readily accessible to the user.

(2) Page Numbers and Revision Data.

(a) The design of the display screen on many video monitors does not allow for complete display of traditional letter size (8.5" x 11") frequently, the video monitor will display only one-third to one-half of a paper page, and the user must scroll the on-screen display to see the complete page. Conversely, some systems will print an entire page even though the video monitor is displaying a partial page. This situation may result in electronic systems assigning, displaying, or printing page numbers that do not match the approved copy of the manual. Therefore, certificate holders and operators must ensure that the information that is displayed or printed can be traced to the correct revision level of the manual.

(b) The contents of a chapter, section, or subject in a maintenance manual may be displayed as a continuous flow of information without the actual page numbers of the approved manual. The user may elect to output only a portion of a manual page containing the relevant information. If this occurs, the organizational format of the manual should be retained, and a means of referencing the section or page of the manual from which the data was obtained should be provided.

(3) References to specific chapters, sections, or paragraphs of the manual may be used to ensure information traceability to corresponding sections of a printed version of the manual. This permits the technical data to be easily referenced by the user and ensures tractability of the information to its source.

(4) The most common method of updating a manual is to issue a revision with a list that identifies the pages to which the revision applies. Each page that is subsequently revised contains the revision status on each page. This same process can be applied when the manuals are in electronic format. The FAA recommends that certificate holders and operators prepare a table of revisions and include that table in the electronic manual to show when each page of the manual was revised.

e. Data Archive. A maintenance recordkeeping requirement frequently requires retention or access to previously used technical data to substantiate a method of repair or maintenance. To facilitate compliance with those tractability requirements, a certificate holder or operator may decide to archive earlier versions of manuals in the event of future need to duplicate, regenerate, or reconstruct maintenance instructions. This archived data may be obtained from the original source of the data. Regardless of the source, the certificate holder or operator is responsible for ensuring the availability of any required record.

(1) Preservation of Stored Data. Procedures should be established by the certificate holder or operator to ensure the integrity of the stored technical data, regardless of the storage medium. These procedures should include:

(a) Ensuring that no unauthorized changes can be made.

(b) Selecting storage mediums that minimize regeneration errors or deterioration.

(c) Exercising, refreshing, or duplicating archived technical data at a frequency compatible with the storage life of the medium (i.e., before deterioration of the storage medium).

(d) Storing duplicate copies in physical separate archives to minimize the risk of data loss in the event of a disaster.

(2) Technology Advances. Certificate holders and operators should ensure that all electronic systems components are maintained so that archived manuals can be retrieved. Future technological advancements in data storage media may result in the replacement of current system hardware or use of another storage medium. Future systems must be able to retrieve the archived technical data, or the certificate holder or operator will have to maintain the old system to ensure data availability.

Nicholas A. Sabatini
Director, Flight Standards Service

APPENDIX 1.
SAMPLE LETTER OF INTENT FOR NON-CERTIFICATE HOLDERS

[*Requester Letterhead*]

To: [*FAA Flight Standards District Office with geographic jurisdiction over the requester's operations*]

From: [*Requester*]

Date: [*Date*]

Subject: Use of Electronic Systems, Recordkeeping/Manuals/Signatures

This letter is to inform you that [*requester non-certificate holder*] intends to use an electronic (recordkeeping and/or manual and/or signatures) system for [*describe what the system will be used for*]. This system has been established using the guidelines outlined in FAA Advisory Circular 120-ES.

This organization intends to implement the system on [*date*].

Company facilities, equipment, and personnel are available for your review and/or inspection at [*address*] on [*date*]. Please contact [*name*] at [*telephone*] to arrange a visit to review the system and to discuss any FAA concerns.

Thank you in advance for your assistance in this matter.

Sincerely,

[Requester]

APPENDIX 2.
SAMPLE LETTER OF FAA ACCEPTANCE FOR NON-CERTIFICATE HOLDERS

Federal Aviation Administration
San Antonio Flight Standards District Office
1992 Barrett Avenue
Travis, Texas 76321

June 2, 2001

Mr. John Smith
ABC Airways, Inc.
1234 South Airport Way
San Antonio, Texas 78910

Dear Mr. Smith:

This letter confirms acceptance of the electronic system used by *[Name]*. The electronic system for (maintenance recordkeeping, manuals, and/or signatures) meets the requirements of Title 14 of the Code of Federal Regulations Part 91.

FAA acceptance is limited to those persons who are trained by *[Name]*, in the use of electronic equipment in accordance with *[Name]*, training programs.

This office should be notified of any significant changes in the design or operation of the system.

The FAA should have access to the system at all times. Any changes to designated FAA user identification codes or passwords should be submitted to the FAA Certificate Holding District Office, as soon as practicable after the change.

Unless sooner withdrawn, this letter is valid for an indefinite period of time.

Sincerely,

Principal Aviation Safety Inspector (Operations and/or Maintenance)